

**BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554**

In the Matter of	)	
	)	
New Part 4 of the Commission's Rules	)	ET Docket No. 04-35
Concerning Disruptions to Communications	)	

TO: The Commission

**REPLY COMMENTS OF THE  
DEPARTMENT OF HOMELAND SECURITY**

The UNITED STATES DEPARTMENT OF HOMELAND SECURITY (DHS), by its attorneys and on behalf of its Directorate for Information Analysis and Infrastructure Protection ("IAIP") and the National Communications System ("NCS"),<sup>1</sup> hereby replies to the comments of other parties in response to the Commission's Notice of Proposed Rule Making in the proceeding captioned above ("Notice").<sup>2</sup>

**I. INTRODUCTION**

As stated in its comments, DHS fully supports the important objectives that the Commission seeks to achieve in the Notice and reiterates its significant interest in, and need for, network outage information across all architectures and telecommunications platforms. Such disruption information is critical to national and homeland security functions central to DHS' mission including planning, incident prevention, impact analysis and mitigation, and improving incident response and recovery.

---

<sup>1</sup> Executive Order No. 12472 of April 3, 1984, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, 49 Fed. Reg. 13471 (1984), established the National Communications System. Executive Order No. 13286 of February 26, 2003, § 46(b), 68 Fed. Reg. 10619, 10627, designated the Secretary of Homeland Security as Executive Agent of the NCS, and it is in that capacity that he submits these comments its on behalf.

<sup>2</sup> *New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, FCC 04-30, released February 23, 2004 (Notice of Proposed Rule Making in ET Docket No. 04-35), summary published at 69 Fed. Reg. 15761 (March 26, 2004) [hereinafter "*Notice*"]. Unless otherwise noted, citations to the *Notice* will be to the FCC document, FCC 04-30. The deadline for filing comments in this proceeding was June 24, 2004. Accordingly, DHS is filing concurrently with these comments, under separate cover, a *Motion to Accept Late-Filed Reply Comments*.

DHS believes, however, that the Commission should modify certain proposals set forth in the Notice in order to balance the needs of the Commission, public, DHS and other government entities (including State and local authorities) and members of industry and create a reporting system that yields timely, complete, reliable, and relevant information. Specifically, DHS continues to have concerns in several key areas:

Foremost among its concerns, DHS continues to urge the Commission to make safeguarding the sensitive information that will be contained in the outage reports a highest priority. The preponderance of comments submitted by other parties demonstrates that this is a widely-held concern. Consonant with the homeland security principles that underlie this proceeding, the Commission should explore all available means to protect sensitive information from inappropriate disclosure to those who might use it to attack the telecommunications infrastructure. Consistent with the agencies' mutual responsibilities under HSPD-7,<sup>3</sup> DHS stands willing to work with the Commission to find a solution that appropriately safeguards the information while meeting the competing needs of all interested parties.

Second, DHS generally shares the Commission's view that a consistent reporting method and metric has merit. However, DHS also believes that significant differences among the various technical platforms that the new rule would encompass require that the common metric be tailored appropriately to ensure that the reporting information obtained from all carriers will be relevant and useful for the analytical purposes to which it will be applied. DHS urges the Commission to evaluate the carriers' various technical arguments on this point very carefully to develop specific metrics that are most appropriate for each platform.

---

<sup>3</sup> See HSPD 7 ¶¶ 6(d), 10 (requiring "Federal departments and agencies [to] appropriately protect information . . . that would facilitate terrorist targeting of critical infrastructure and key resources . . .").

Finally, DHS believes that the procedural and physical processes for reporting must be simple, secure and efficient. The processes should give due consideration to the concerns expressed by service providers relative to the economic and administrative costs of the proposals in the Notice while balancing the need to have the needed information readily available to the Commission, DHS, and State and local entities.

## **II. THE COMMISSION SHOULD INCLUDE IN THE RULES ADOPTED IN THIS PROCEEDING APPROPRIATE PROVISIONS TO SAFEGUARD SENSITIVE NETWORK OUTAGE INFORMATION AGAINST INAPPROPRIATE DISCLOSURE OR USE.**

In its comments, DHS urged the Commission that any expansion of the outage reporting rules adopted in this proceeding be accompanied by appropriate measures to safeguard reporting data to the maximum extent consistent with applicable information access laws.<sup>4</sup> DHS observed that the outage data to be reported includes detailed cause and impact information that, in the hands of hostile actors, could be employed to target and attack the nation's critical communications infrastructure.<sup>5</sup> Numerous commenters spanning the market segments impacted by the Commission's proposed rules expressed similar grave concerns about the risks presented by making the reporting information publicly accessible and urged the Commission to take steps to protect the information.<sup>6</sup>

DHS also observed in its comments that arguments supporting greater protection for the reporting data might be attenuated if public accessibility of the information was necessary to

---

<sup>4</sup> Comments of the Department of Homeland Security ("DHS Comments") at 14.

<sup>5</sup> *Id.*

<sup>6</sup> See Comments of AT&T Corp. at 29-30; Comments of BellSouth Corporation at 27-28; Comments of T-Mobile at 17-19; Comments of Sprint Corporation at 27-28; Comments of MCI, Inc. at 6-7; Comments of Qwest Communications International Inc. at 24-25; Comments of SBC Communications at 22-23; Comments of Globalstar LLC at 5-8; Comments of Iridium Satellite LLC at 8; Comments of the Alliance for Telecommunications Industry Solutions at 33-34 ("ATIS Comments"); see also Comments of CTIA at 9-11; Comments of the United States Telecom Association at 24-25 ("USTA Comments").

achieve the benefits identified by the Commission in the Notice.<sup>7</sup> However, as DHS also noted, this is not the case. As SBC Communications notes: “It is not public access, but cooperative analysis of the data and studies . . . that have led to a greater understanding of network reliability issues and the development of Best Practices.”<sup>8</sup>

The reporting of outage information, coupled with the voluntary NRIC processes, has led to a significant strengthening of our nation’s networks. In the past two sessions of NRIC, over 400 best practices covering all telecommunications platforms have been developed including consideration of both physical and cyber homeland security needs. The expansion of outage reporting to all platforms will serve to augment the voluntary NRIC and NRSC processes.

Moreover, as DHS previously observed, the NCC Telecom-ISAC and NCS’ Network Security Information Exchange (“NSIE”) also now provide a forum – unavailable when the reporting rules were first adopted – to enable members of industry to share information with one another and with Government experts on both anomaly and systemically based vulnerabilities and to support the development of best practices.<sup>9</sup> With the expansion of reporting in a post 9/11 environment it is essential that information be protected from broad public release while insuring that key stake holders, *e.g.*, the Commission, DHS, State and Local organizations, and members of industry have access for assessment and planning purposes.

DHS recognizes that not all information to be reported is sensitive. For example, service providers routinely provide press releases during major outages and some of the information requested under the proposals in the Notice would be considered non-sensitive. It may be

---

<sup>7</sup> DHS Comments at 15.

<sup>8</sup> SBC Comments at 22.

<sup>9</sup> DHS Comments at 17.

desirable, if efficient, to split access to information reported into public and sensitive data with processes providing for secure access.<sup>10</sup>

DHS is willing to work collaboratively with the Commission to explore this and other possibilities to determine the most effective means consistent with existing information access laws to protect the information. Several commenters took notice of DHS' authority under Section 214 of the Homeland Security Act<sup>11</sup> to provide such protection to critical infrastructure information under certain circumstances.<sup>12</sup> In its own comments, DHS also noted this authority<sup>13</sup> and is prepared to explore with the Commission whether and how the Protected Critical Infrastructure Information Program could be employed to safeguard outage reporting information.

### **III. DHS SUPPORTS A CONSISTENT REPORTING METHODOLOGY THAT PROVIDES THE INFORMATION NEEDED TO SUPPORT ONGOING IMPROVEMENTS IN NETWORK RELIABILITY AND ENABLES EFFECTIVE PLANNING FOR PREVENTION, IMPACT MITIGATION AND RESTORATION.**

While generally supporting the consistent reporting concept advanced by the Commission, DHS, in its comments, questioned whether the “common metric” proposed in the Notice was suitable for application to all of the platforms that will be affected by the new reporting rule.<sup>14</sup> DHS urged the Commission to consider modifying the common metric as may be appropriate for specific platforms to ensure that information ultimately reported by affected carriers is relevant and useful for its intended applications.

---

<sup>10</sup> Sprint appears to envision a similar approach in its comments. *See* Sprint Comments at 28 (suggesting that “the Commission ‘scrub’ reports of critical network information before allowing public access to the reports.”); *see also* Qwest Comments at 25.

<sup>11</sup> 6 U.S.C. § 133.

<sup>12</sup> *See* AT&T Comments at 29; MCI Comments at 7.

<sup>13</sup> DHS Comments at 10 n.22.

<sup>14</sup> *Id.* at 16.

In their comments, numerous service providers and vendors have identified significant differences among the various telecommunications platforms, architectures, size of carriers, and business model that impact the utility of the proposed user minute metric. It appears to DHS that many of these arguments have merit and require thoughtful analysis (*e.g.*, use of numbers of access lines proposed by ATIS). DHS again urges the Commission to review carefully the alternative formulations proposed by the various carriers relative to the reporting metric to be employed for each platform. In the end, application of the most appropriate metric, if not necessarily the most uniform one, will be critical to achieve the objective of the Notice: obtaining the most accurate, relevant, and complete information possible in the most effective and efficient manner.

**IV. THE REPORTING PROCESSES MUST BE CLEAN, SIMPLE AND SECURE WITH A FOCUS ON THE VALUE OF INFORMATION FOR PLANNING PURPOSES AND EMPHASIS ON A PRIORITY FOR RESTORATION ACTIVITIES.**

As mentioned above, information, especially, sensitive data, must be available in a timely fashion to all major stakeholders including the Commission, DHS, State and local governments and industry. A key here is timeliness. As ATIS and CTIA both note, in an outage situation the first priority must be to get the network(s) operational and the personnel responsible for reporting are usually the same personnel responsible for restoration.<sup>15</sup>

DHS agrees with this priority and supports the recommendation to revise the proposed reporting scheme to allow for a three phased reporting process – 120 minutes to report the outage, 72 hours for the first detailed report and 30 days for the final report. DHS believes that existing operational processes for coordination at the national level through the NCS' NCC and similar processes at the State and local level will provide maximum opportunity to understand

---

<sup>15</sup> ATIS Comments at 31; CTIA Comments at 15.

and effectively execute response and recovery activities. The information provided to all stakeholders will still fully support the planning and improvement processes for enhancing prevention, impact mitigation, and response programs at all levels.

A number of commenters expressed significant concern over the economic and administrative impacts that the proposed reporting process and reporting requirements would have on multiple organizations and locations. USTA suggests that a central repository accessible by all Federal, State, local, and industry stakeholders would provide a clean and efficient manner for public and sensitive/secure data access.<sup>16</sup> DHS supports this concept and submits that the NCC could serve as an appropriate point for managing such a repository.

## **V. CONCLUSION**

With the conditions set forth in its original comments and the above reply comments DHS continues its support of this NPRM and recognizes its value to support the planning for National and Homeland security requirements for prevention, impact mitigation, response preparation and development of critical services to meet its missions. DHS reiterates that the implementation procedures and processes must meet the needs of all stakeholders at the Federal, State and local levels and preserve the strong partnerships we have with industry. Further, all data is not needed by the public and all data and information of a sensitive nature must be defined and protected. There are opportunities to insure the processes are effective and efficient

---

<sup>16</sup> USTA Comments at 11.

and DHS stands prepared to work collaboratively with the Commission and other stakeholders, as the Commission deems appropriate, to address these matters.

Respectfully submitted,

**UNITED STATES DEPARTMENT OF  
HOMELAND SECURITY**

By: /s/ Joe D. Whitley  
Joe D. Whitley  
General Counsel  
United States Department of Homeland Security  
701 D Street, S.W.  
Washington, D.C. 20528  
(202) 692-4232

/s/ Thomas J. Connelly  
Thomas J. Connelly  
Associate General Counsel for  
Information Analysis and Infrastructure Protection  
United States Department of Homeland Security  
Nebraska Avenue Complex  
Washington, D.C. 20528  
(202) 692-4232

/s/ Eric T. Werner  
Eric T. Werner  
United States Department of Homeland Security  
700 D Street, S.W.  
Washington, D.C. 20528  
(202) 401-0775

Date: June 29, 2004